

کمپیوٹر سیکورٹی۔۔ حصہ اول

احتیاط کے حوالے سے کچھ ضروری باتیں: یہ احتیاطی تدابیر اس لئے بتائی جا رہی ہیں تاکہ جو لوگ جہاد سے اور مجاہدین سے محبت رکھنے والے ہیں وہ ایجنسی والوں کی خبیث نظر سے محفوظ رہیں، کیونکہ یہی جہاد سے محبت رکھنے والے اس امت کا سرمایہ ہیں اور آگے جاکہ انہی کو بڑے کام سرانجام دینے ہونگے تو کیوں ابھی سے احتیاط شروع نہ کریں، ابھی سے اگر احتیاط نہیں کریں گے تو آپ ان ایجنسیوں کی نظر میں ہونگے اور آگے جاکر اگر آپ کوئی کام کرنا چاہیں بھی تو نہیں کر سکیں گے، کیونکہ یہ دشمن بہت مکار ہے اس کی زندہ مثال یہ ہے کہ ابھی جب پشاور کے اسکول کا واقعہ ہوا تو اس کے رد عمل میں کراچی کے مدرسوں سے سوسے زائد طلباء کو ان ایجنسی والوں نے اٹھایا اور اکثر کودو، تین دن میں ہی شہید کر کے لاش چھینک دیا اور نام پولیس مقابلے کا لگا دیا۔ تو کیا ان سب کو اٹھانا ایک ہی دن کی معلومات کے ذریعے کیا؟ نہیں بلکہ ان کے فون کالز کے ذریعے اور دوسرے جاسوسی کے طریقے سے ان کا معلوم کیا، ان کا جرم بھی صرف اتنا ہی تھا کہ یہ مجاہدین سے محبت رکھنے والے تھے اور کچھ بھی نہیں کیا تھا انہوں نے۔ یہ ایجنسی والے اسی طرح مجاہدین سے محبت رکھنے والوں کو اپنی نظر میں رکھتے ہیں اور ایسا واقعہ ہو جائے تو اس کے رد عمل میں انہی کو شہید کرتے ہیں کیونکہ ان کا ہاتھ تو دھرم تک ہی پہنچتا ہے۔ اور پچھلے سال کے فیسبک کار یا پورٹ ہے کہ پاکستانی حکومت نے صرف 6 مہینے میں 160 اکاونٹس کے ڈیٹا مانگے ہیں اور 1600 کے قریب مواد اور اکاونٹ ہلاک کرنے کا درخواست کیا۔ اس سے آپ اندازہ لگا سکتے ہیں کہ دشمن آپ کے خلاف کتنے منصوبے کر رہا ہے اور آپ کی غفلت ان کو فائدہ پہنچائیگی۔ ایسا نہ ہو کہ صرف جہاد سے محبت کرنے کی وجہ سے آپ کو اس کی سزا بھگتنی پڑے۔

اب فیصلہ آپ نے کرنا ہے کہ آپ نے احتیاط کرنا ہے یا نہیں، ہمارا کام تو صرف بات پہنچانا ہے باقی آپ کی مرضی ہے کہ آج سے احتیاط شروع کرنی ہے اور ان باتوں سے فائدہ اٹھانا ہے یا پھر زندگی میں کہیں ٹھوکر کھا کر صرف افسوس ہی کرنا ہے، اُس وقت کا افسوس پھر کچھ فائدہ نہیں دیگی، اس لئے بہتر یہ ہے کہ آپ ابھی سے احتیاط کو اپنے زندگی کا لازمی حصہ بنالیں، یقیناً اُس احتیاط میں بھی آپ کو صبر کے مراحل سے گزرنا ہوگا، انٹر نیٹ کی اسپید سست ہوگی، اور ان کو اختیار کرنے میں بھی کافی وقت صرف ہوگا مگر یہ کل کے افسوس سے بہتر ہے۔

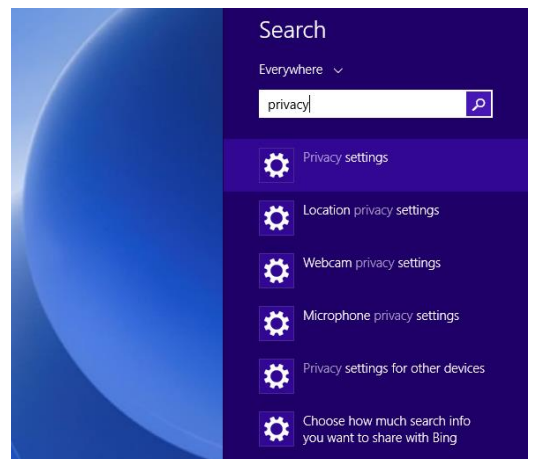
لیکن یہ بات بھی ذہن میں رہے کہ حفاظت کرنے والا تو اللہ ہی ہے اور اس نے ہمیشہ اپنے بندوں کی حفاظت فرمائی ہے، جدید ترین ٹیکنالوجی بھی مجاہدین کا کچھ نہیں بگاڑ سکیں۔ مگر جو اسباب اللہ تعالیٰ نے ہمارے لئے مہیا کئے ہیں ہم ان اسباب کو اختیار کریں اور اللہ پر توکل کریں۔ جب اسٹریلیا، امریکہ، فرانس میں مجاہدین کے کاروائیاں ہوتی ہیں اور ادھر کی ایجنسی ان کا سراغ نہیں لگا سکتے تو ہماری ایجنسی جو کہ ان کا غلام ہے ہر لحاظ سے وہ کیا خاک معلوم کرے گا۔ بس ہم غلطیاں نہ کریں، احتیاط کریں اور اصل کام اللہ پر توکل کریں تو یہ ہمارا کچھ نہیں بگاڑ سکتے۔ اور وہ فیسبوک والی رپورٹ میں ہے تھا کہ پاکستانی حکومت نے ان کے ڈیٹا کی جھیک لگوائی ہے مگر یہ نہیں بتایا کہ کیا انہوں نے اس جھکاری کو ان کے ڈیٹا دیئے بھی ہیں یا نہیں۔ البتہ دوسرے ممالک کے ساتھ فیسبوک والے تعاون کرتے ہیں اور ڈیٹا فراہم کرتے ہیں، جیسے ابھی حال ہی میں ایک خبر آئی تھی کہ ایٹنڈیا کی پولیس کے ساتھ واٹس ایپ اور فیسبوک والے تعاون کر رہے ہیں اور انہی کے تعاون سے ایٹنڈیا کی پولیس نے حزب المجاہدین کے کچھ لوگوں کو مارا تھا۔

اور آخری چیز "دعاء انس رضی اللہ عنہ" کے پڑھنے کو اپنا معمول بنائیں۔

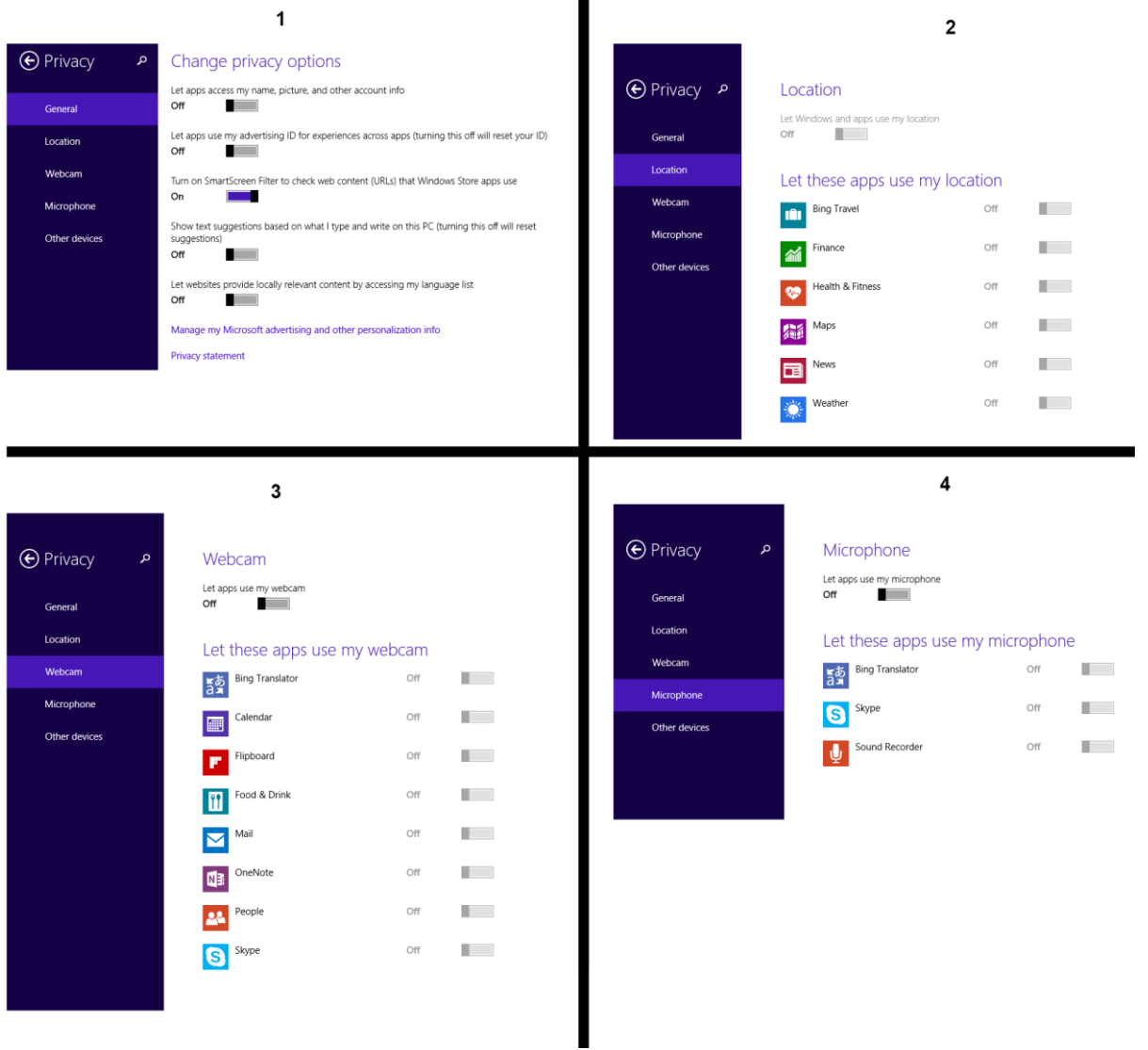
وینڈوز کی سیکیورٹی:

کمپیوٹر میں جتنا نیا یا پیڈیا آپریٹنگ سسٹم مثلاً وینڈوز، لینکس وغیرہ استعمال کریں اتنا ہی بہتر ہے۔ ویسے تو لینکس کی سیکيورٹی وینڈوز سے کافی بہتر ہے مگر چونکہ اکثریت وینڈوز ہی استعمال کرتی ہے، اس لئے اس سیکیشن میں ہم کمپیوٹر میں صرف وینڈوز سے متعلق بات کریں گے۔ چونکہ لینکس کا استعمال کرنے والے کمپیوٹر میں پہلے سے مہارت رکھتے ہیں ان کو ان باتوں کی ضرورت بھی نہیں ہوگی، رہی بات میک / Mac استعمال کرنے والوں کی وہ اس سے اندازہ لگا کر بھی اپنے سیکيورٹی سخت کر سکتے ہیں۔

۱۔ **Windows 8** یا اس سے اوپر والوں میں لوکیشن وغیرہ کو بند کرنا: سب سے پہلے search میں جائیں اور وہاں Privacy settings پر اس پر کلک کریں جیسا تصویر میں دکھایا ہے۔



پھر اس میں سیننگلز کو ایسا کرس جیسے نیچے تصویر میں دکھایا ہے۔ یعنی General میں سب کو Off کرس سوائے Smart Screen Filter کو۔



Location پہ کلک کریں اور اس کو Off کریں۔

پھر webcam پہ کلک کریں اور اسے بھی Off کریں۔ اگر آپ Skype وغیرہ استعمال کرتے ہوں تو صرف استعمال کرتے وقت ان کو On کریں۔

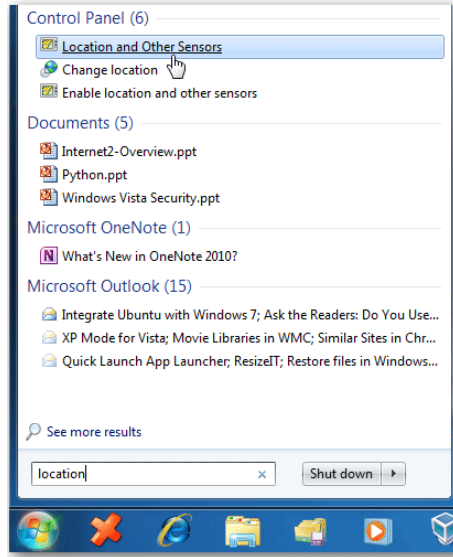
پھر Microphone پہ کلک کریں اور Off کریں۔

نوٹ: جو لوگ مجاہدین سے رابطے میں ہیں اور ان سے مدد وغیرہ بھی کرتے ہیں، یعنی میڈیم اور ہائی پروفائل کے لوگ صرف ان سینٹرز پہ اکتفاء نہ کریں بلکہ اپنے لپ ٹاپ کے ویب کیمرہ پہ ٹیپ لگائیں۔ اور اسپیکر کے خانے میں ایئر فون ڈالیں اور آپشن میں مانک سیلکٹ کریں، تاکہ لپ ٹاپ کا مانک کام نہ کرے۔

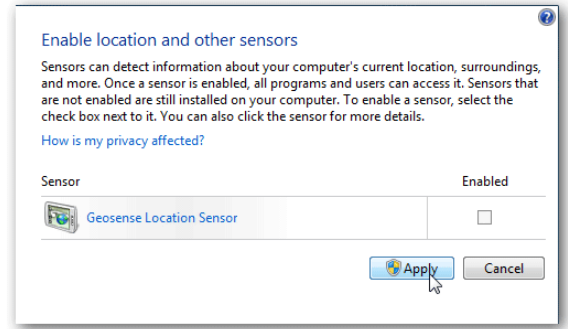
Windows 7 میں ان سینٹرز کا طریقہ: ویڈیوز 7 میں یہ سینٹرز تو موجود نہیں البتہ کسی کسی میں لوکیشن کی سینٹرز ہیں۔

اس کے لئے آپ پہلے Start پہ کلک کریں Search خانے میں لکھیں Location، پھر Location and Other Sensors پہ کلک کریں

1



2



اگر Geosense Location Sensor پہ Enabled پہ صحیح کا نشان نہیں لگا تو رہنے دیں اگر لگا ہے تو اسے ختم کر دیں اور پھر Apply پہ کلک کریں۔

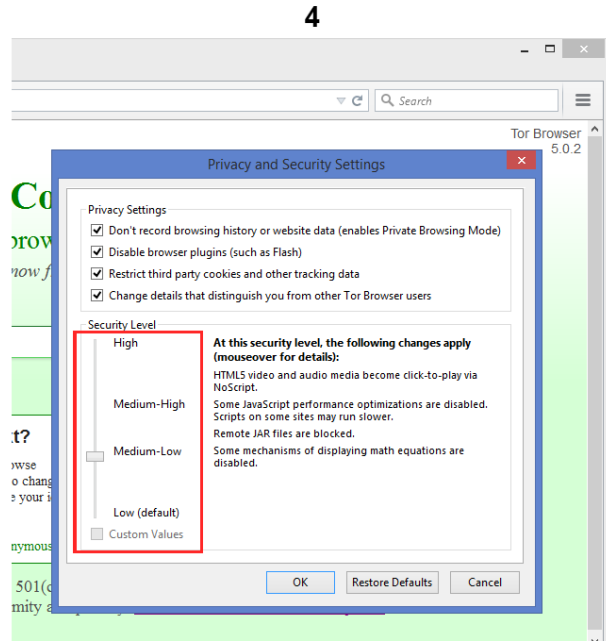
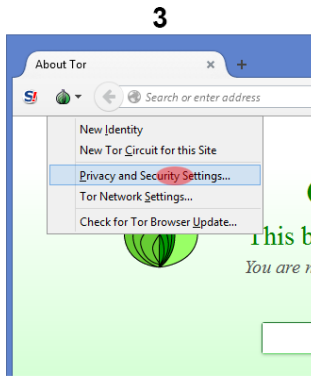
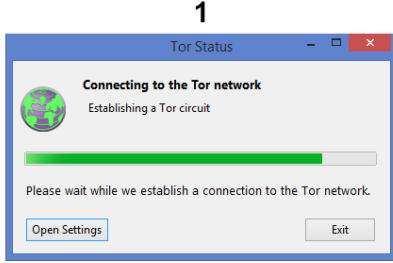
ضروری نہیں کہ یہ آپشن وینڈوز 7 کے سب ورژن میں ہو، یہ کسی ورژن میں ہوتا ہے۔

بروزر کے سینکڑوں بروزر کا انتخاب

TOR: یہ سب سے زیادہ محفوظ بروزر و محفوظ پراکسی (آئی پی ایڈریس تبدیل کرنے کا) سافٹ ویئر ہے۔ اس کو یہاں سے ڈاؤن لوڈ کریں:

<https://www.torproject.org/download/download-easy.html.en>

ڈاؤن لوڈ کر کے انسٹال کریں، اور اس کو چلائیں۔ یہ اسکرین آؤٹ۔

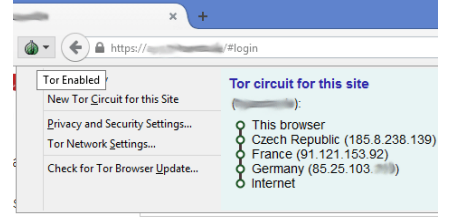


جیسا تصویر میں دکھایا ہے شروع میں یہ اسکرین آؤٹ یعنی Tor کنفیگ ہو رہا ہے، پہلی مرتبہ تھوڑا دیر کر کے بعد میں پھر جلدی کھلیگا، پھر جب کنفیگ ہو جائیگا تو تصویر ۲ جیسا اسکرین آؤٹ یعنی اب یہ بروزر Tor پہ چل رہا ہے اب اس کا استعمال کر سکتے ہیں۔

اس میں سیکیورٹی کو مزید سخت کرنے کیلئے نیاز والے نشان پہ کلک کریں جیسا تصویر ۲ میں دکھایا ہے۔ پھر Privacy and Security Settings پہ کلک کریں۔

پھر سیکیورٹی لیول کو دیکھیں جس قدر آپ سیکیورٹی دینا چاہتے ہیں دے دیں، جتنا بڑھائینگے ویب سائٹ اتنا سستی سے کھلیں گے اور بعض ویب سائٹ صحیح نہیں کھلیں گے تو عام طور پر Medium Low پہ رکھیں۔

نوٹ: ویسے عام طور پر Low پر ہوتی ہے اور اگر اس کے اس سینکڑوں کو تبدیل نہ بھی کریں تب بھی صحیح ہے۔ Low پہ بھی ہو تو تب بھی سیکیورٹی سخت ہی ہوتی ہے کیونکہ ٹور ایک برج سے دوسرے اور دوسرے سے تیسرے پہ اور پھر انٹرنیٹ کا استعمال کرتی ہے جیسا اس تصویر میں دکھایا ہے



اور براؤزر کو بھی اپنے سکیورٹیز سینکڑوں پر رکھتی ہے، یہ مزید سکیورٹی ان کی لئے ہے جو بڑے ہیکرز سے بچنا چاہتے ہیں، اور ایسے ہیکرز پاکستان میں تو مشکل ہے ایسے ہوں۔ اس لئے Medium Low پر رکھیں زیادہ مناسب ہے اور اگر Medium Low پر بھی کوئی ویب سائٹ صحیح نہیں کھل رہا اور آپ کو وہ چلانا ہو تو آپ Low پر ہی رکھیں کوئی مسئلہ نہیں۔ ٹور کی سکیورٹی باقی عام پر کسی سافٹوئیر سے ۱۰ گنا بہتر ہے۔

Tor سے محفوظ طریقے سے فیسبوک استعمال کرنے کے لئے یہ لنک استعمال کریں: <https://www.facebookcorewwwi.onion>

اس لنک کا فائدہ یہ ہے کہ اس سے آپ کی کوئی بھی آئی پی ایڈریس فیسبوک والوں کے پاس نہیں جاگی، نہ اصلی اور نہ پر کسی والی۔ یہ ٹور ہی کے سرور کے ذریعے فیسبوک استعمال کرتی ہے۔ اگر آپ اس کا کنکٹ ہونے کا ڈانگر ام دیکھیں تو اس طرح نظر آئے گا کہ ایک برج سے دوسرے برج، دوسرے سے تیسرے پھر ریلے کا استعمال ہو گا جن میں ایک ریلے سے دوسرے، دوسرے سے تیسرے اور پھر فیسبوک۔ ریلے کے ذریعے فیسبوک کے پاس آئی پی ایڈریس نہیں جاگی۔

اس کا فائدہ یہ ہے کہ عام طور پر جب آپ مختلف ممالک کے آئی پی ایڈریس استعمال کرتے ہیں تو فیسبوک آپ کو بلاک کرتی ہے اور کچھ سکیورٹی سوال کرتی ہے اور بعض اوقات بغیر سوال کہ صرف آئی ڈی کارڈ اپلوڈ کا کہتی ہے جس سے یقینی طور پر فیسبوک کا بلاک کرنا ہی مراد ہے۔ تو اس لنک کے ذریعے سے استعمال کرنے میں آپ کو کوئی مسئلہ پیش نہیں آئے گا اگر فیسبوک آگے کوئی اقدام نہ کرے تو۔

عام براؤزر میں آپ اس لنک میں نہیں جاسکتے۔

ہمیشہ Tor کا پبلیڈٹ ورژن استعمال کریں، اور اپڈیٹ کرتے رہیں۔

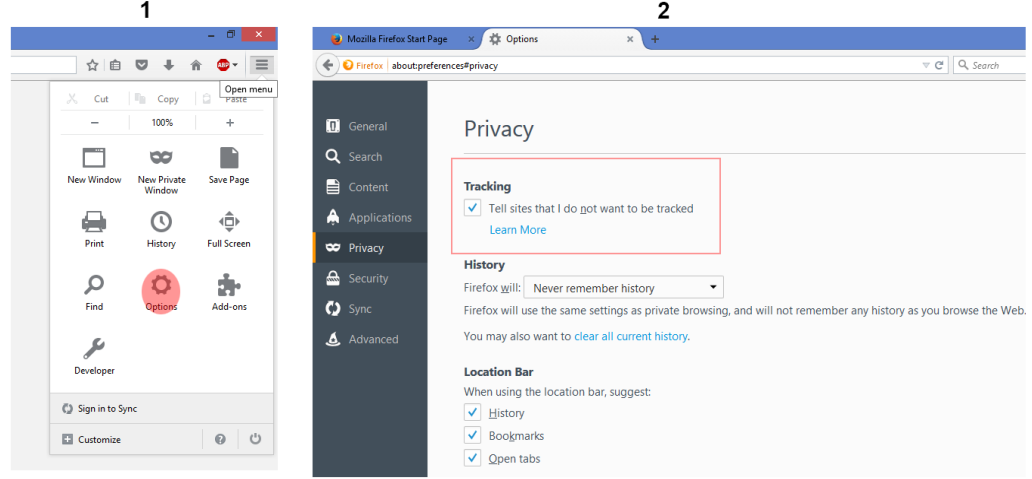
ایک شبہ اور اس کا جواب: یہاں یہ سوال پیدا ہو سکتا ہے کہ TOR یہ سب کچھ مفت میں کیوں دے رہی ہے حالانکہ دوسرے پر کسی سافٹوئیر تو پیسے لے کر بھی کم سکیورٹی دیتے ہیں، اور ٹور کس طرح کمائی کرتی ہے؟ تو اس کا جواب یہ ہے کہ ٹور کو ایک امریکی ادارے نے بنایا تھا اور وہی اس کو فنڈنگ کرتے تھے اور یہ لوگوں کے ڈونیشن یعنی چندے بھی لیتی ہے، بڑے بڑے ادارے بھی ان کو بہت زیادہ ڈونیشن دیتے ہیں اس سروس فراہم کرنے کے بدلے۔ ان سب کا مقصد بھی یہی ہے کہ لوگوں کی پرائیویسی/رازداری محفوظ رکھنے کیلئے ان کو یہ سروس مفت میں ملے۔ اور ٹور کو ان ڈونیشن/چندے سے اتنے پیسے ملتے ہیں شاید دوسرے پر کسی سافٹوئیر والوں کو پیسے پہنچنے پر بھی نہیں ملتے۔ البتہ ایک شبہ یہ ہو سکتا ہے کہ اس کو سب سے زیادہ فنڈنگ امریکی ایک ادارہ کر رہا ہے تو کیا یہ ان کیلئے جاسوسی نہیں کر سکتی؟ تو اس میں یہ بتانا چلوں کہ جتنے بھی ہیکرز ہیں ان میں سے اکثریت ٹور پر بھروسہ کرتے ہیں اور یہ بھروسہ اس کو آزمانے کے بعد ہی کرتے ہیں، چونکہ بلیک ہیٹ ہیکرز بھی اپنے اپنے ممالک کے سکیورٹی اداروں سے یا سی آئی اے سے چھپے ہوتے ہیں، ان کا بھی جرم بہت بڑا ہوتا ہے اور وہ ٹور ہی استعمال کرتے ہیں۔ تو ہم ان کے تجربے پر تھوڑا بہت بھروسہ کر سکتے ہیں۔ البتہ مکمل بھروسہ اس پہ بھی نہیں ہو سکتا۔

نوٹ: بعض حضرات zenmate کا استعمال کرتے ہیں اور دوسروں کو مشورہ بھی دیتے ہیں، تو اس کے متعلق بتانا چلوں چونکہ وہ بھی مفت سروس فراہم کر رہا ہے مگر اس کا مقصد آپ کی لاگ کو امریکہ کی ایجنسی کو پہنچانا ہی ہے، اس پر بقاعدہ تحقیق ہوئی ہے۔ لہذا اس کو استعمال نہ کریں۔ اور دوسرے اس طرح کے مفت سروس دینے والوں کو بھی استعمال نہ کریں جب تک تحقیق نہ کریں۔ اور ایک بات کہ جو سافٹوئیر کریک ہوئے ہوں وہ دراصل مفت نہیں ہیں، بلکہ ان کو ہیک کر کے مفت بنایا جاتا ہے، اس لئے ان کو مفت نہ سمجھیں۔

دیگر براؤزر کے سینکڑ

اگر آپ کے نیٹ کاسپیڈ سست ہے اور TOR چلانے میں مشکل ہو رہی ہو تو آپ F Secure Freedom F انشال کر کے (انشال کرنے کا طریقہ آگے بتائیے) اس کے ساتھ فائرفاکس یا کروم یا اوپرا کا استعمال کریں، تینوں کی اپنی اپنی خوبیاں اور خامیاں ہیں البتہ Firefox بہتر ہے۔

افائرفاکس / Firefox: سب سے پہلے لوکیشن ٹریس ہونے والے آپشن کو ختم کریں، اس کیلئے یہ تصویر دیکھیں۔



یعنی پہلے براؤزر کے مینیو میں جائیں پھر اس میں Options کو کلک کریں، پھر اس میں سے Privacy کو کلک کریں پھر Tracking والے آپشن میں دیکھیں اس آپشن کو صحیح کا نشان لگائیں جیسا تصویر ۲ میں دکھایا ہے۔

اگر آپ مزید احتیاط کرنا چاہتے ہیں تو ای سینکڑز میں History کو Never remember history پہ سیلکٹ کریں ویسے اس سے بہتر طریقہ یہ ہے کہ آپ Private window کھولیں۔

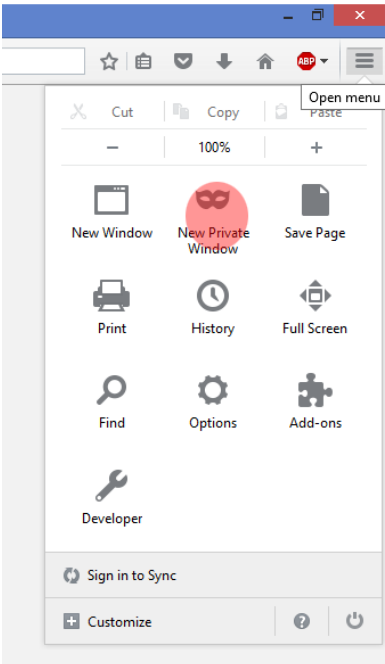
اس کا طریقہ یہ ہے آپ براؤزر کے مینیو میں جائیں، پھر اس میں New Private window پہ کلک کریں۔

اس میں یہ ہوتا ہے کہ اس سے آپ کا براؤزر اس کی ہسٹری، پاسورڈ، کوکیز، ٹیمپیری فائلز وغیرہ کچھ بھی محفوظ نہیں کرتا۔

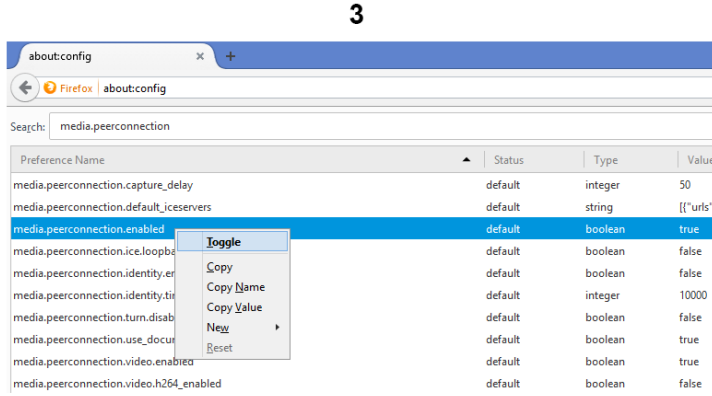
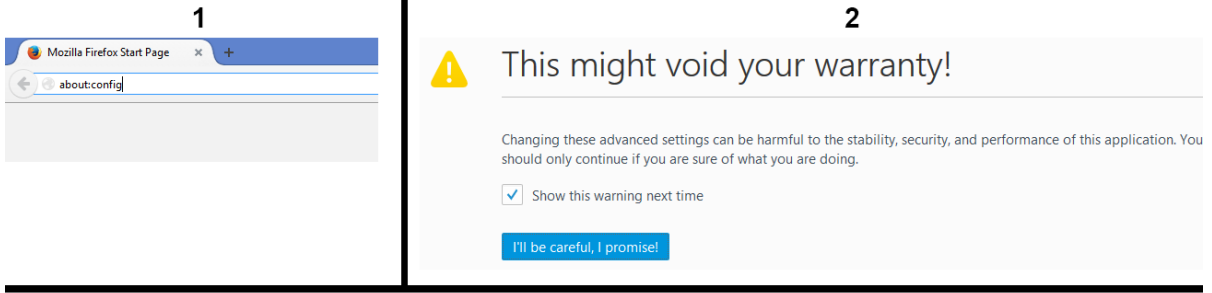
اس سے آپ کسی حد تک محفوظ رہتے ہیں۔ مگر اس سے ویب سائٹ تھوڑا سستی سے کھلیں گے کیونکہ دوسرے طریقے سے جب آپ ایک ویب سائٹ کو دوسری مرتبہ کھولتے ہیں تو وہ ٹیمپیری فائلز کو لوڈ کرتا ہے جو پہلے محفوظ ہو چکے ہیں اور اس طرح ویب سائٹ جلد کھل جاتا ہے، مگر اس طریقے سے ہر بار اس کو اس ویب سائٹ کے تمام فائل لوڈ کرنے پڑتے ہیں۔

ایک براؤزر پر کئی فیسبوک اکاؤنٹ کھولنے کیلئے بھی یہ طریقہ مفید ہے، یعنی ایک اکاؤنٹ کھولا اور پھر لوگ آؤٹ ہوئے پھر اسی براؤزر پر دوسرا اکاؤنٹ کھولا، اس کیلئے یہ طریقہ استعمال کریں کیونکہ دوسرے طریقے سے پھر فیسبوک آپ کو سیکیورٹی سوال کر سکتا ہے کیونکہ اس سے آپ مشکوک ہوتے ہیں کہ ایک ہی براؤزر سے کئی اکاؤنٹ۔ اور فیسبوک ڈاریکٹ کو کیزن تک رسائی حاصل کرتی ہے اگر پہلے موجود ہوں۔ اس طرح آپ نے اگر ایک فیک اکاؤنٹ بنایا ہے اور ایک اصل اکاؤنٹ ہے تو فیسبوک کو پتا چل جاتا ہے کہ یہ ایک ہی کمپیوٹر سے استعمال ہو رہا ہے اور ایک ہیکر آسانی سے معلوم کر سکتا ہے۔ اس لئے بہتر یہ ہے کہ فیسبوک کیلئے Private window کا انتخاب کریں اگر Tor استعمال نہیں کرتے۔

اور براؤزر پہ کبھی بھی پاسورڈ محفوظ ہونے والے آپشن کو کلک مت کریں۔



WebRTC: فائر فوکس سے ویب آر ٹی سی یعنی پراکسی لگانے کے بعد اپنا اصلی آئی پی ایڈریس ظاہر ہونے والے خلاء کو بند کرنے کا طریقہ یہ ہے کہ آپ فائر فوکس کو کھولیں اور ویب سائٹ کے کانے میں یہ لکھیں



About:config اور انٹر کریں، پھر ایک اسکرین آؤٹ جیسا تصویر ۲ میں دکھایا ہے، اس میں I'll be carefull والے آپشن کو کلک کریں

پھر ایک اسکرین آؤٹ کی اس میں سرچ کی جگہ یہ لکھیں media.peerconnection.enabled پھر اس میں دیکھیں اس نام والے خانے میں اگر value true لکھا ہوگا پھر اس کو رائٹ کلک کر کے Toggle پہ کلک کریں اب اس میں False لکھا آئیگا۔ اب اس کو بند کر کے دوبارہ اسٹارٹ کریں۔ اور یہ چیک کرنے کیلئے کہ واقعی بند ہو گیا ہے آپ اس لنک پہ جائیں۔

<https://diafygi.github.io/webrtc-ips/>



اگر اس طرح کا اسکرین آؤٹ یعنی Ip addresses پہ خالی ہو تو Webrtc بند ہو چکا ہے۔ اگر آئی پی ظاہر ہو تو بند نہیں ہوا ہے دوبارہ سے سیٹنگز دیکھ لیں اور اسے بند کر دیں۔

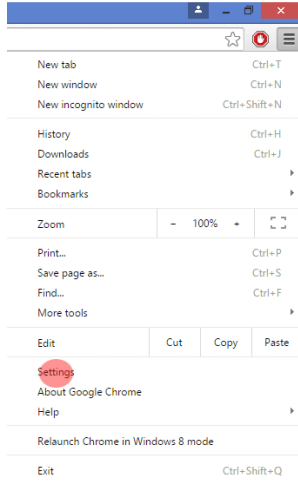
Adblock: اپنے براؤزر میں ایڈ بلاک پلگ ان ضرور ڈالیں، یہ Ads کو بلاک کرتی ہے اور اکثر ایڈز میں ایسے اسکرپٹ ہوتے ہیں جو لوکیشن معلوم کرتے ہیں۔ اور اس سے آپ کافی حد تک جاسوسی سافٹ ویئر کے

خود کار انسٹال ہونے سے بھی بچ سکتے ہیں۔ اس لنک پہ جائیں <https://addons.mozilla.org/en-US/firefox/addon/adblock-plus>

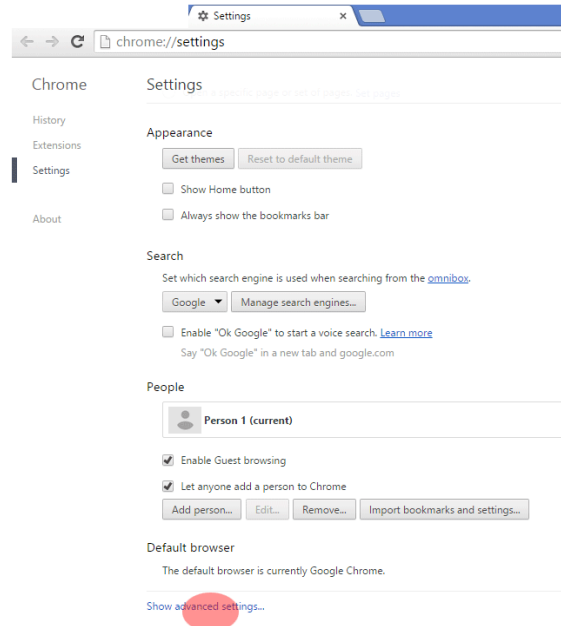
اس پہ جا کہ دیکھیں Add to firefox لکھا آئیگا، اس پہ کلک کریں، یہ اس میں انسٹال ہو جائیگا۔

Google Chrome: اس میں بھی پہلے لوکیشن ٹریس والے آپشن کو ختم کریں۔ اس کیلئے آپ براؤزر کھولیں، مینیو میں جائیں پھر اس میں سینکڑوں میں جائیں

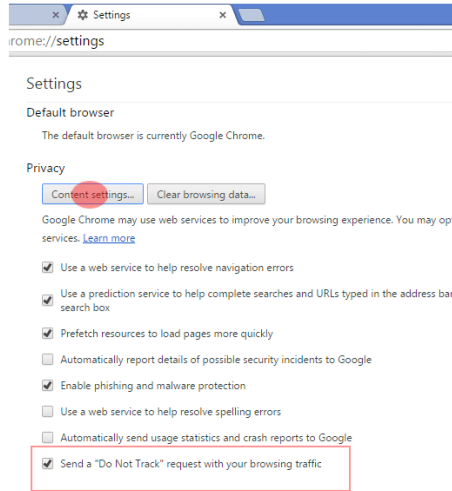
1



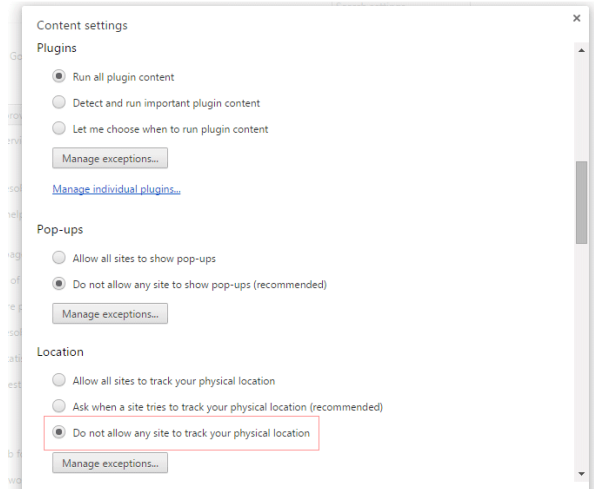
2



3



4



پھر نیچے جائیں اور Show advanced settings پہ کلک کریں، پھر اس میں نیچے دیکھیں Send a Do not track والے آپشن کو صحیح کا نشان لگائیں جیسا تصویر دس میں دکھایا ہے
پھر Privacy کے نیچے Content Settings پہ کلک کریں اس میں نیچے جائیں لوکیشن والے خانے میں دیکھیں Do not allow any site آپشن کو سیلک کریں۔

گوگل کروم میں Private window کا نام incognito ہے، اور اس کیلئے مینیو میں جائیں جیسا تصویر 1 میں دکھایا ہے اس میں New Incognito window پہ کلک کریں۔ اور پرائیویٹ ویڈو کی تفصیل فائر فاکس کے ذیل کرچکا ہوں۔ اسے ضرور پڑھیں۔

WebRTC: گوگل کروم میں webrtc کو مکمل ختم نہیں کر سکتے مگر کسی حد تک بند ہو جاتی ہے اس پلگ ان سے، اس لنک پہ جائیں اور پلگ ان ڈاؤن لوڈ کر کے کروم میں ڈال دیں۔

<https://chrome.google.com/webstore/detail/webrtc-leak-prevent/eiadekoaikejlgdbkdbfeijglgfdalm1?hl=en>

اور چیک کرنے کیلئے اسی لنک پہ جائیں: <https://diafygi.github.io/webrtc-ips/>

Adblock: اس لنک پہ جا کہ Add to chrome پہ کلک کریں:

<https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnlbpbkdaibdcddilifddb>

Opera: اوپر ایس لوکیشن ٹریس والے آپشن کو ختم کرنے کیلئے اس کو کھولیں پھر اس میں اوپر کونے میں opera لکھا ہو گا اس کو کلک کریں

پھر Settings پہ کلک کریں

پھر اس میں Privacy & Security پہ کلک کریں۔

پھر اس میں Send a Don't track والے آپشن کو صحیح کا نشان لگائیں۔

Private window کیلئے opera والے آپشن کو کلک کریں اور new private window پہ کلک کریں۔

WebRTC: اوپر ایس بھی webrtc کو مکمل بند نہیں کر سکتے بس Noscript lite پلگ ان ڈال کر کسی حد تک روک سکتے ہیں۔ اس پلگ ان کا لنک:

<https://addons.opera.com/en/extensions/details/noscript-lite/?display=en>

Adblock: اس لنک پہ جا کہ Add to opera پہ کلک کریں:

<https://addons.opera.com/en/extensions/details/opera-adblock/?display=de>

F Secure Freedom

اگر Tor سٹ ہو اور اسے استعمال کرنے میں دشواری ہو رہی ہو تو خصوصی رابطے کیلئے پھر بھی وہی استعمال کریں اور عام براؤزنگ پھر ایف سکیور فریڈوم سے کریں۔ ایف سکیور فریڈوم باقی پر کسی سافٹویر سے کافی بہتر ہے۔

ایف سکیور فریڈوم ویسے 14 دن ٹرائل ورژن کے ساتھ آتا ہے مگر اس کو اس طریقے سے ڈاؤنلوڈ کرنے سے اور کوڈ ڈالنے سے آپ کو 180 دن یعنی ۶ مہینے کے لئے استعمال کرنے کی اجازت دیتا ہے۔ طریقہ یہ ہے:

پہلے اس لنک پہ جائیں:

https://campaigns.f-secure.com/freedom/chip/de_DE

یہ جرمن زبان میں ہے اس لئے یہ تصویر دیکھیں اور اس پر عمل کریں

پہلے خانے یعنی Kampagnencode میں آپ یہ کوڈ ڈالیں **FRDECHQ3**

دوسے خانے میں آپ اپنا ای میل ایڈریس دیں جہاں آپ ای میل میں کوڈ وصول کر سکتے ہوں

تیسرے خانے یعنی Sprache میں زبان کا انتخاب کریں English کا، چونکہ یہ جرمن زبان

میں ہے اس لئے اس میں English لکھا ہوگا اس کو سیلکٹ کریں پھر نیچے ویریفیکیشن کوڈ کو

لکھیں اور پھر Absenden پہ کلک کریں۔

پھر آپ کو ایک کوڈ ایگ میل میں اس کو فریڈوم میں ڈالنا ہوگا۔

فریڈوم کا ڈاؤنلوڈ لنک:

[https://download.sp.f-](https://download.sp.f-secure.com/freedom/installer/Freedom.exe)

[secure.com/freedom/installer/Freedom.exe](https://download.sp.f-secure.com/freedom/installer/Freedom.exe)

ڈاؤنلوڈ کرنے کے بعد کھولیں اور سبک پرپشن پہ کلک کر کہ کوڈ ڈالیں جو آپ کو میل میں آیا تھا، اس سے

آپ اس کو 180 دن کیلئے استعمال کر سکتے ہیں۔

اسے On کرنے کیلئے Off پہ کلک کریں جب On نظر آئے تو یہ چل رہا ہے۔ لوکیشن تبدیل کرنے کیلئے لوکیشن پہ کلک کر کہ کوئی سالو کیشن سیلکٹ کر سکتے ہیں، بہتر یہی ہے کہ بار بار تبدیل کریں۔ بس فیسبوک

کیلئے ایک ہی ملک کا استعمال کریں کیونکہ اس سے آپ کا اکاؤنٹ بند ہو سکتا ہے۔

نوٹ: یہ سافٹویر جولا گزرد کھاتی ہے مثلاً کہ اتنا ڈیٹا انکرپٹ کیا ہے، اتنے ویب سائٹ بلاک کئے ہیں، اتنے ٹریکنگ حملے روکے ہیں، یہ سب غلط دکھاتی ہیں اس لئے ڈرنے کی ضرورت نہیں کہ کوئی آپ پہ اتنے ٹریکنگ کرنا

چاہ رہا ہے، اور یہ ٹریکنگ بھی اکثر ایڈز کے ذریعے سے ہی ہوتے ہیں۔

Antivirus

اپنے کمپیوٹر میں اینٹی وائرس ضرور ڈالیں۔ ایک اچھے اینٹی وائرس کا انتخاب آپ کو %80 ہیکنگ سے محفوظ رکھتا ہے۔ ہیکنگ اور ہیکنگ سے بچنے کے بارے میں اگلے ٹورنیل میں بتائیں گے ان شاء اللہ۔

سب سے بہترین اینٹی وائرس Bitdefender ہے۔ اس کو آپ Torrent سے ڈاؤنلوڈ کر سکتے ہیں۔ ٹول سیکیورٹی ڈاؤنلوڈ کریں۔ کیونکہ اس کا فری ورژن 15 یا 30 دن کیلئے ہوتا ہے، ٹورنٹ سے آپ کو اس کا کریک ورژن ملیگا۔ ایک لنک یہ ہے:

<https://kat.cr/bitdefender-total-security-2015-build-18-21-0-1497-x86-x64-incl-trial-reset-keys-b-tman-t10267276.html>

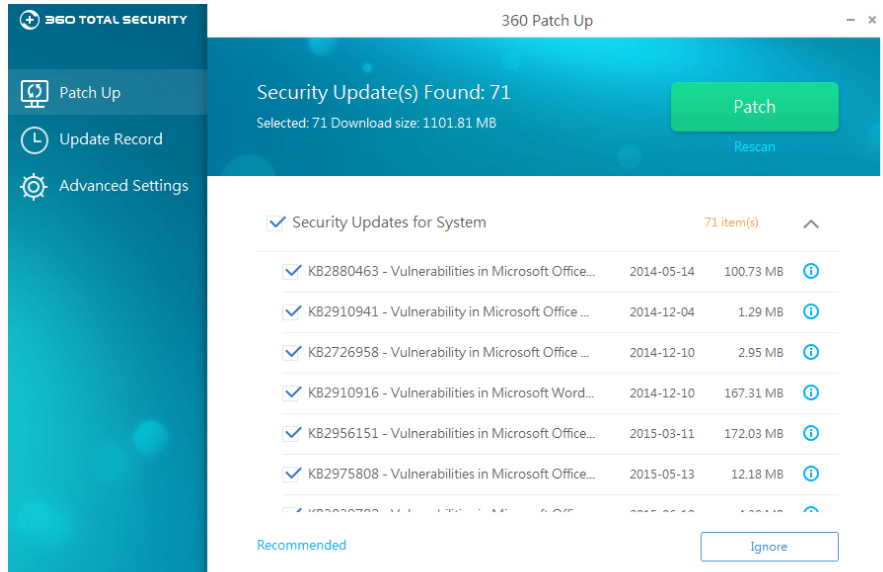
اس میں جو نسا ورژن آپ ڈاؤنلوڈ کرنا چاہتے ہیں وہ سیلکٹ کریں یعنی 32bit یا 64bit، اس میں دونوں موجود ہیں آپ ان میں سے ایک کو سیلکٹ کریں ڈاؤنلوڈ کرنے کیلئے جو نسا آپ کا وینڈوز ہو۔ ہر ایک 300mb ہے۔ اس میں انسٹال نوٹس کو پڑھ کر انسٹال کریں۔

سست کمپیوٹر والوں کیلئے متبادل: اگر آپ کا سسٹم سست ہے اور ایسا اینٹی وائرس برداشت نہیں کر سکتا تو آپ Qihoo 360 Total Security ڈاؤنلوڈ کر کے انسٹال کریں۔ یہ بہت ہلکا ہے اور سیکیورٹی بھی اچھی ہے۔ اس کو آپ یہاں سے ڈاؤنلوڈ کر سکتے ہیں۔

<http://www.360totalsecurity.com/en/download-free-antivirus/360-total-security/?offline=1>

اس کو ڈاؤنلوڈ کر کے انسٹال کریں۔ اس کا پڑیٹ ہونے کا طریقہ یہ ہے کہ یہ آپ کے سسٹم کو اسکن کر کے دیکھے گا کہ کون کون سے سافٹوئیر انسٹال ہیں اور ان سافٹوئیر کیلئے کون سے ضروری فائل انسٹال کرنے ہوں گے۔

اس کا طریقہ یہ ہے کہ آپ اسے کھولیں، اس میں آپ Tool Box کو کھولیں پھر اس میں Patch Up پہ کلک کریں۔ اسکن کر کے آپ کو اس طرح کا لسٹ آئیگا۔



اگر آپ سب کو ایک ساتھ ڈاؤنلوڈ نہیں کر سکتے تو آپ ایک ایک کو سیلکٹ کر کے بھی کر سکتے ہیں، بس جس کو ڈاؤنلوڈ کرنا ہے اسے سیلکٹ کریں اور Patch پہ کلک کریں۔

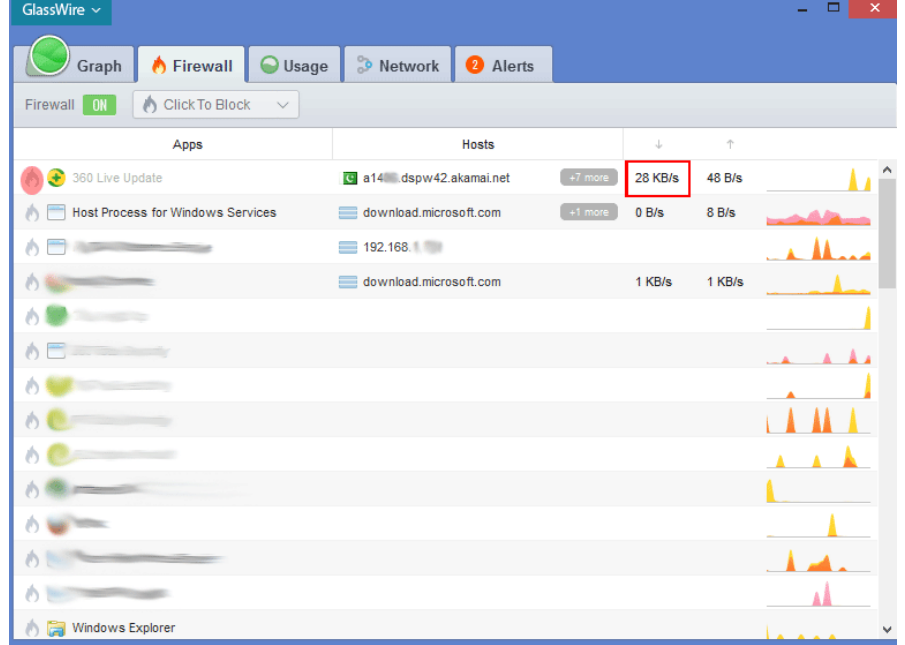
نوٹ: یہاں بھی وہی سوال پیدا ہو سکتا ہے کہ باقی اینٹی وائرس تو مفت نہیں ملتے یہ کیوں مفت ہے، تو یہ بتانا چلوں کہ یہ سافٹوئیر چائنا کی کمپنی Qihoo کی ہے، اور چائینا والے کمپنیوں کا مقصد یہ ہے کہ دوسرے امریکی کمپنیوں کا مقابلہ کرنے کے لئے لوگوں کو مفت سروس فراہم کرو۔ اور شاید آگے جا کر جب مارکیٹ میں نام کمالیں اور جگہ حاصل کر لیں پھر اسی کا Pro ورژن متعارف کروائیں۔

اینٹی وائرس جو نسا بھی ڈالیں پہلے فل سسٹم اسکن کریں۔ اینٹی وائرس کو اپڈیٹ کرتے رہیں۔

فائر وال / Firewall

فائر وال ایک ایسا سافٹ ویئر ہے جس سے آپ دوسرے سافٹ ویئر کو انٹرنیٹ استعمال کرنے کی اجازت اور منع کر سکتے ہیں، اور انٹرنیٹ ٹریفک کی مکمل نگرانی کر سکتے ہیں۔ اس سے آپ جاسوسی سافٹ ویئر کو بھی دیکھ سکتے ہیں، آگے بتانگے کہ کیسے۔

بہتر یہ ہے کہ آپ اسی 360 Total Security کا فائر وال ڈاؤن لوڈ کریں۔ اس کیلئے آپ وہ اینٹی وائرس کھولیں اور اس میں Tool Box پہ کلک کریں، پھر اس میں Firewall پہ کلک کریں، وہ بیک گراؤنڈ میں ڈاؤن لوڈ ہو کہ انسٹال ہو گا۔ اس کے فائر وال کا نام GlassWire ہے۔ اب آپ اسے کھولیں



Firewall والے ٹیب کو کھولیں، اس میں سافٹ ویئر کی لسٹ ہو گی جو انٹرنیٹ استعمال کر رہے ہیں، آپ جس کو چاہیں انٹرنیٹ استعمال کرنے سے منع کر سکتے ہیں اس کیلئے اس سافٹ ویئر کے سامنے آگ والے نشان کو کلک کریں جیسا تصویر میں دکھایا ہے۔ اور یہ بھی دیکھ سکتے ہیں کہ کونسی آئی پی استعمال ہو رہی ہے، جیسا اس تصویر میں پاکستان کے جھنڈے کا نشان ہے یعنی پاکستان کی آئی پی ایڈریس استعمال ہو رہی ہے۔ اور کونسا سافٹ ویئر کتنا ڈیٹا استعمال کر رہا ہے یہ بھی آپ دیکھ سکتے ہیں۔

اور کس سافٹ ویئر نے کتنا ڈیٹا استعمال کیا ہے وہ دیکھنے کیلئے آپ Usage والے ٹیب پہ کلک کریں اور دیکھیں۔

جاسوسی سافٹ ویئر کا اس طرح پتہ چلے گا کہ وہ یہاں ڈیٹا استعمال کر رہا ہو گا، آپ دیکھیں کہ جس سافٹ ویئر کو آپ نہیں جانتے اور وہ ویبڈوز کا بھی نہیں ہے تو ممکن ہے کہ وہ جاسوسی سافٹ ویئر ہو، مگر ایسے کمزور جاسوسی سافٹ ویئر کو یہ اینٹی وائرس خود ہی سراغ لگا نہ گا۔۔۔۔

نوٹ: یہ اتنا ہم نہیں ہے، اگر کسی کا کمپیوٹر سست ہے تو وہ یہ نہ ڈالے۔ ویسے تو ویبڈوز کا اپنا فائر وال بھی ہوتا ہے اور دوسرے بڑے اینٹی وائرس میں یہ چیز موجود ہے۔

اگلے ٹور نیل میں ہیٹنگ سے متعلق کچھ باتیں ہونگی، اور اس کیلئے کچھ احتیاطی تدابیر بتائیں گے، اور فیسبک کے اکاؤنٹ ہیک ہونے سے بچانے کیلئے احتیاطی تدابیر بھی بتائیں گے۔

کسی بھی قسم کا کوئی مشورہ یا معلومات شیئر کرنی ہو تو آپ ہمیں ضروری میل کریں۔

اپنے دعاؤں میں یاد رکھیے گا

والسلام علیکم

ای میل ایڈریس: abuturab@tutanota.com

ویب سائٹ: besafer.wordpress.com